2:25mj173 CMR

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Collin Scott, being duly sworn, hereby depose and state that the following is true to the best of my information, knowledge, and belief:

INTRODUCTION AND AGENT BACKROUND

1. I have been employed as a Special Agent of the FBI since January 2018, and am currently assigned to the Salt Lake City Field Office and FBI Child Exploitation Task Force. Prior to my employment with the FBI, I obtained a Bachelor's degree in Information Technology, and was employed with a computer software company for five years. As a result of my training and experience, I am familiar with information technology and its use in criminal activities. Since joining the FBI, I have investigated violations of federal law, and am currently investigating federal violations concerning child pornography and the sexual exploitation of children.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

PURPOSE OF THE AFFIDAVIT

3. This affidavit is submitted in support of an application to search a Motorola cellular phone belonging to Jason Knudsen and currently in the possession of the Utah County Jail, (the "Subject Phone"), further described in **Attachment A**, for the items described in **Attachment B**, which are evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) (Receipt and Distribution of Child Pornography) and (a)(5)(B) (Possession of or Access with Intent to View Child Pornography) (the "Subject Offenses").

5. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause for the requested warrant.

6. The information contained within the Affidavit is based on my training and experience, as well as information imparted to me by other law enforcement officers involved in this investigation.

BRIEF SUMMARY

7. As set forth in detail below, the FBI is investigating registered sex offender Jason Knudsen for crimes related to the distribution of child pornography. In February, 2005, federal search warrants were obtained for Knudsen's home and person. The search warrant on his home was executed on February 18, 2025, and child pornography was found. However, the search warrant on Knudsen's person was not executed, because it was discovered that Knudsen had been arrested on February 13, 2025, by the American Fork Police Department on unrelated charges and was still in state custody. At the time of his arrest, he was in possession of the Subject Phone. He was booked into the Utah County Jail; the Subject Phone is currently there, with his personal property. Knudsen was interviewed at the jail; he admitted to collecting child pornography on his laptop. He said law enforcement could search the Subject Phone, but would not find anything. The phone has not yet been searched.

8. For the above reasons and others noted in this Affidavit, I believe there is probable cause to search the Subject Phone for evidence of the Subject Offenses.

DEFINITIONS

9. The following definitions apply to this Affidavit and **Attachment B** to this Affidavit:

10. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

11. "Visual depictions" includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

12. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

13. "IP Address" means Internet Protocol address, which is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

14. "Internet" means a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

15. In this Affidavit, the terms "computers" or "digital storage media" or "digital storage devices" may be used interchangeably, and are intended to include any physical object upon which computer data can be recorded as well as all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices capable of performing logical, arithmetic, or storage functions, including desktop and laptop computers, mobile phones, tablets, server computers, game consoles, network hardware, hard disk drives, RAM, floppy disks, flash memory, CDs, DVDs, and other magnetic or optical storage media.

SEIZURE AND SEARCH OF COMPUTERS

16. As described above and in **Attachment B**, I submit that if computers or storage media are found at the Subject Premises**,** there is probable cause to search and seize those items for the reasons stated below. Some of these electronic records might take the form of files, documents, and other data that is user-generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis. They may be seized and searched on-scene, and/or searched off-scene in a controlled environment.

17. For example, based on my knowledge, training, and experience, I know that a powered-on computer maintains volatile data. Volatile data can be defined as active information temporarily reflecting a computer's current state including registers, caches,

physical and virtual memory, network connections, network shares, running processes, disks (floppy, tape and/or CD-ROM), and printing activity. Collected volatile data may contain such information as opened files, connections to other computers, passwords used for encryption, the presence of anti-forensic tools, or the presence of programs loaded in memory that would otherwise go unnoticed. Volatile data and its corresponding evidentiary value is lost when a computer is powered-off and unplugged.

18. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

19. Also, again based on my training and experience, wholly apart from user-generated files, computer storage media contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, virtual memory "swap" or paging files, and shadow copies of previous versions of systems or files, or paging files. Computer users typically do not erase

or delete this evidence because special software is typically required for that task. However, it is technically possible to delete this information. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted, edited, moved, or show a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

20. As further described in **Attachment B**, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how computers were used, why they were used, the purpose of their use, and the purposes to which they were put, who used them, the state of mind of the user(s), and when they were used.

21. The monitor and printer are also essential to show the nature and quality of the images or files that the system can produce. In addition, the analyst needs all assisting software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices. Moreover, searching computerized information for evidence or instrumentalities of crime commonly requires the seizure of the entire computer's

input/output periphery devices (including related documentation, passwords and security devices) so that a qualified expert can accurately retrieve the system's data in a controlled environment.

22. The computer and its storage devices, the mouse, the monitor, keyboard, printer, modem and other system components are also used as instrumentalities of the crime to operate the computer to commit offenses involving the sexual exploitation of minors. Devices such as modems and routers can contain information about dates, IP addresses, MAC addresses, frequency, and computer(s) used to access the Internet or to otherwise commit the crimes described herein. The computer equipment may also have fingerprints on them indicating the user of the computer and its components.

23. Information or files related to the crimes described herein are often obtained from the Internet or the cellular data networks using application software which often leaves files, logs or file remnants which would tend to show the identity of the person engaging in the conduct as well as the method of location or creation of the images, search terms used, exchange, transfer, distribution, possession or origin of the files. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

24. "User attribution" evidence can also be found on a computer and is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, videos, and correspondence (and the data associated with the foregoing, such as file creation and last accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time. For example, I know from training and experience that persons trading in, receiving, transporting, distributing or possessing images involving the sexual exploitation of children or those interested in the firsthand sexual exploitation of children often communicate with others through correspondence or other documents which could tend to identify the origin and possessor of the images as well as provide evidence of a person's interest in child pornography or child sexual exploitation. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

25. I know from training and experience that digital software or hardware exists that allows persons to share digital access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address. Examination of these items can reveal information about the authorized or unauthorized use of Internet connection at the residence.

26. Searching computer(s) for the evidence described in **Attachment B** may require a range of data analysis techniques. For example, information regarding user attribution or

Internet use is located in various operating system log files that are not easily located or reviewed. Or, a person engaged in criminal activity will attempt to conceal evidence of the activity by "hiding" files or giving them deceptive names. As explained above, because the warrant calls for records of how a computer has been used, what it has been used for, and who has used it, it is exceedingly likely that it will be necessary to thoroughly search storage media to obtain evidence, including evidence that is not neatly organized into files or documents. Just as a search of a premises for physical objects requires searching the entire premises for those objects that are described by a warrant, a search of this premises for the things described in this warrant will likely require a search among the data stored in storage media for the things (including electronic data) called for by this warrant. Additionally, it is possible that files have been deleted or edited, but that remnants of older versions are in unallocated space or slack space. This, too, makes it exceedingly likely that in this case it will be necessary to use a multitude of techniques, both on and off-scene, including more thorough techniques.

27. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes involving child exploitation, they should all be seized as such.

28. Based upon my knowledge, training and experience, I know that a thorough search for information stored in digital storage media requires a variety of techniques, that often includes both on-site seizure and search as well as a more thorough review off-site review in a controlled environment. This variety of techniques is required, and often agents must seize most or all storage media to be searched on-scene and/or later in a controlled environment. These techniques are often necessary to ensure the accuracy and completeness

of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction.

29. For example, the search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following on-site techniques (the following is a non-exclusive list, as other on-site search procedures may be used):

A. On-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;

B. On-site copying and analysis of volatile memory, which is usually lost if a computer is powered down, and may contain information about how the computer is being used, by whom, when, and may contain information about encryption, virtual machine software (virtual operating systems that are lost if the computer is powered down or encrypted),;

C. On-site forensic imaging of any computers may be necessary for computers or devices that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for any examination.

30. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include off-site techniques since it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined off-site and in a controlled environment. This is true because of the following:

A. The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how, when and why a computer has been used, by whom, what it has been used for, requires considerable time, and taking that much time on premises could be unreasonable. Also, because computer evidence is extremely vulnerable to tampering and destruction (both from external sources and from code embedded in the system as a "booby-trap"), the controlled environment of a laboratory may be essential to its complete and accurate analysis. Searching for and attempting to recover any deleted, hidden, or encrypted data may be required to determine whether data falls within the list of items to be seized as set forth herein (for example, data that is encrypted and unreadable may not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of child exploitation offenses).

B. The volume of evidence and time required for an examination. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse

all the stored data to determine which particular files are evidence or instrumentalities of crime. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Reviewing information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

C. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

D. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

E. Need to review evidence over time and to maintain entirety of evidence. I recognize the prudence requisite in reviewing and preserving in its original form

only such records applicable to the violations of law described in this Affidavit and in **Attachment B** in order to prevent unnecessary invasion of privacy and overbroad searches. I advise it would be impractical and infeasible for the Government to review the mirrored images of digital devices that are copied as a result of a search warrant issued pursuant to this Application during a single analysis. I have learned through practical experience that various pieces of evidence retrieved from digital devices in investigations of this sort often have unknown probative value and linkage to other pieces of evidence in the investigation until they are considered within the fluid, active, and ongoing investigation of the whole as it develops. In other words, the weight of each individual piece of the data fluctuates based upon additional investigative measures undertaken, other documents under review and incorporation of evidence into a consolidated whole. Analysis is content-relational, and the importance of any associated data may grow whenever further analysis is performed. The full scope and meaning of the whole of the data is lost if each piece is observed individually, and not in sum. Due to the interrelation and correlation between pieces of an investigation as that investigation continues, looking at one piece of information may lose its full evidentiary value if it is related to another piece of information, yet its complement is not preserved along with the original. In the past, I have reviewed activity and data on digital devices pursuant to search warrants in the course of ongoing criminal investigations. I have learned from that experience, as well as other investigative efforts, that multiple reviews of the data at different times is necessary to understand the full

value of the information contained therein, and to determine whether it is within the scope of the items sought in **Attachment B**. In order to obtain the full picture and meaning of the data from the information sought in **Attachments A and B** of this application, the Government would need to maintain access to all of the resultant data, as the completeness and potential of probative value of the data must be assessed within the full scope of the investigation. As such, I respectfully request the ability to maintain the whole of the data obtained as a result of the search warrant, and to maintain and to review the data in the control and custody of the Government and law enforcement at times deemed necessary during the investigation, rather than minimize the content to certain communications deemed important at one time. As with all evidence, the Government will maintain the evidence and mirror images of the evidence in its custody and control, without alteration, amendment, or access by persons unrelated to the investigation.

31. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for permits both on-site seizing, imaging and searching as well as off-site imaging and searching of storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later and perhaps repeated examination consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

[32. Purposefully left blank]

33. I know from training and experience that digital storage devices can be very large in capacity, yet very small in physical size. Additionally, I know from training and experience that those who are in possession of such devices also tend to keep them on their persons, especially when they may contain contraband or other evidence of a crime. The storage capacity of such devices can be as large as tens of gigabytes in size as further described below, which allows for the storage of thousands of images and videos as well as other digital information such as calendars, contact lists, programs and text documents. Such storage devices can be smaller than a postage stamp in size, which allows them to be easily hidden in a person's pocket.

BACKGROUND REGARDING THE INTERNET AND CHILD EXPLOITATION

34. I have a Bachelor's degree in Information Technology, and worked cyber-criminal investigations as an FBI Agent for six years, so I am familiar with computers and their use in crimes. I also own my own computer, have personal knowledge of the operation of a computer, and have accessed the Internet for numerous years. Based on this training and knowledge, and the experience of other law enforcement personnel involved in this investigation, I know the following:

35. Child pornographers can produce images using a wireless device such as a cell phone. Photos can also be made using cameras, then can be transferred onto another device either using wire or wireless technology. Images can also be uploaded to Internet-based storage commonly referred to as the "cloud." Hard-copy images can also be scanned into a computer. Via the Internet, connection can be made to literally millions of computers around the world. Child pornography can be transferred quickly and easily via electronic mail or

virtually countless other online platforms, communication services, storage services, and applications.

36. A computer's capability to store images in digital form makes it an ideal repository for child pornography and other files related to the sexual abuse and exploitation of children. The digital-storage capacity in devices and in the "cloud" has grown tremendously within the last several years. Thumb drives with a capacity of 128 GB are not uncommon. Flash cards with a capacity of 64 gigabytes are not uncommon. Hard drives with the capacity of 500 gigabytes up to 3 terabytes are not uncommon. Phones with over 100 gigabytes in storage are not uncommon. Devices can store thousands of images and videos at very high resolution. These devices are often internet capable and can not only store, but can transmit images via the internet and can use the devices to store images and documents in internet or "cloud" storage spaces. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

37. With Internet access, a computer user can transport an image file from the Internet or from another user's computer to his own computer, so that the image file is stored in his computer. The process of transporting an image file to one's own computer is called "downloading". The user can then display the image file on his computer screen, and can choose to "save" the image on his computer and/or print out a hard copy of the image by using a printer device (such as a laser or inkjet printer). Sometimes the only method to recreate the evidence trail of this behavior is with careful laboratory examination of the computer, modem, printer, and other electronic devices.

38. I know from training and experience that search warrants of residences involved in computer or digitally related criminal activity usually produce items that tend to establish ownership or use of digital devices, and ownership or use of any Internet service accounts accessed to obtain child pornography to include credit card bills, telephone bills, correspondence and other identification documents.

39. I know from training and experience that search warrants of residences usually reveal items that tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.

THE USE OF PEER-TO-PEER FILE SHARING SOFTWARE TO DISTRIBUTE CHILD PORNOGRAPHY ON THE BITTORRENT NETWORK

40. Millions of computer users throughout the world use peer-to-peer (P2P) file sharing networks to share files containing music, graphics, movies and text. These networks have also become a popular way to download and distribute child pornography. Any computer user who can connect to the internet can download P2P application software, which is typically free, and use it to share files through a P2P network.

41. The BitTorrent network is a very popular and publicly available P2P file sharing network. Most computers that are part of this network are referred to as "peers" or "clients". A peer/client can simultaneously provide files to some peers/clients while downloading files from other peers/clients.

42. The BitTorrent network can be accessed by peer/client computers via many different BitTorrent network client (software) programs, examples of which include the

BitTorrent client program, uTorrent client program, and Vuze client program, among others. These client programs are publicly available and typically free P2P client software programs that can be downloaded from the Internet.

43. During the installation of typical BitTorrent network client programs, various settings are established which configure the host computer to share files via automatic uploading.[1] Typically, as users download files or pieces of files from other peers/clients on the BitTorrent network, other users (peers/clients) on the network are able to download the files or pieces of files from them, a process which maximizes the download speeds for all users on the network. Once a user has completed the download of an entire file or files, they can also continue to share the file with individuals on the BitTorrent network who are attempting to download all pieces of the file or files, a process referred to as "seeding".

44. Files or sets of files are shared on the BitTorrent network via the use of "Torrents". A "Torrent" is typically a small file that describes the file(s) to be shared. It is important to note that "Torrent" files do not contain the actual file(s) to be shared, but information about the file(s) to be shared needed to accomplish a download. This information includes things such as the name(s) of the file(s) being referenced in the

[1] As an example, during the downloading and installation of the publicly available uTorrent client program, the license agreement for the software states the following: "Automatic Uploading. uTorrent accelerates downloads by enabling your computer to grab pieces of files from other uTorrent or BitTorrent users simultaneously. Your use of the uTorrent software to download files will, in turn, enable other users to download pieces of those files from you, thereby maximizing download speeds for all users. In uTorrent, only files that you are explicitly downloading or sharing (seeding) will be made available to others. You consent to other users' use of your network connection to download portions of such files from you. At any time, you may uninstall uTorrent through the Add/Remove Programs control panel utility. In addition, you can control uTorrent in multiple ways through its user interface without affecting any files you have already downloaded, thereby maximizing download speeds for all users.

"Torrent" and the "info hash" of the "Torrent". The "info hash" is a SHA-1[2] hash value of the set of data describing the file(s) referenced in the "Torrent". This set of data includes the SHA-1 hash value of each file piece in the torrent, the file size(s), and the file name(s). The "info hash" of each "Torrent" uniquely identifies the "Torrent" file on the BitTorrent network. The "Torrent" file may also contain information on how to locate file(s) referenced in the "Torrent" by identifying "Trackers". "Trackers" are computers on the BitTorrent network that collate information about the peers/clients that have recently reported they are sharing the file(s) referenced in the "Torrent" file. A "Tracker" is only a pointer to peers/clients on the network who may be sharing part or all of the file(s) referenced in the "Torrent". "Trackers" do not actually have the file(s) but are used to facilitate the finding of other peers/clients that have the entire file(s) or at least a portion of the file(s) available for sharing. It should also be noted that the use of "Tracker(s)" on the BitTorrent network are not always necessary to locate peers/clients that have file(s) being shared from a particular "Torrent" file. There are many publicly available servers on the Internet that provide BitTorrent tracker services.

45. In order to locate "Torrent" files of interest and download the files that they describe, a typical user will use keyword searches on torrent indexing websites, examples of

[2] The Secure Hash Algorithm (SHA) was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), as a means of identifying files using a digital "fingerprint" that consists of a unique series of letters and numbers. The United States has adopted the SHA1 hash algorithm described herein as a Federal Information Processing Standard. SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols. A file processed by this SHA1 operation results in the creation of an associated hash value often referred to as a digital signature. SHA1 signatures provide a certainty exceeding 99.99% that two or more files with the same SHA1 signature are identical copies of the same file regardless of their file names.

which include isohhunt.com and the piratebay.org. Torrent indexing websites are essentially search engines that users on the BitTorrent network use to locate "Torrent" files that describe the files they are looking to download. Torrent indexing websites do not actually host the content (files) described by "Torrent" files, only the "Torrent" files themselves. Once a "Torrent" file is located on the website that meets a user's keyword search criteria, the user will download the "Torrent" file to their computer. The BitTorrent network client program on the user's computer will then process that "Torrent" file in order to find "Trackers" or utilize other means that will help facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the "Torrent" file. It is again important to note that the actual file(s) referenced in the "Torrent" are actually obtained directly from other peers/clients on the BitTorrent network and not the "Trackers" themselves. Typically, the "Trackers" on the network return information about remote peers/clients that have recently reported they have the same file(s) available for sharing (based on SHA-1 "info hash" value comparison), or parts of the same file(s), referenced in the "Torrent", to include the remote peers/clients Internet Protocol (IP) addresses.

46. For example, a person interested in obtaining child pornographic images or videos on the BitTorrent network can go to a torrent indexing website and conduct a keyword search using a term such as "preteen sex" or "pthc" (pre-teen hardcore). The results of the keyword search are typically returned to the user's computer by displaying them on the torrent indexing website. Based on the results of the keyword search, the user would then select a "Torrent" of interest to them to download to their computer from the website. Typically, the BitTorrent client program will then process the "Torrent" file. Utilizing trackers and other BitTorrent network protocols, peers/clients are located that have recently reported they have

the file(s) or parts of the file(s) referenced in the "Torrent" file available for sharing. The file or files are then downloaded directly from the computer(s) sharing the file or files. Typically, once the BitTorrent network client has downloaded part of a file or files, it may immediately begin sharing the part of the file or files it has with other users on the network. The BitTorrent network client program succeeds in reassembling the file(s) from different sources only if it receives "pieces" with the exact SHA-1 hash value of that piece which is described in the "Torrent" file. The downloaded file or files are then stored in an area (folder) previously designated by the user and/or the client program on the user's computer or designated external storage media. The downloaded file or files, including the torrent file, will remain in that location until moved or deleted by the user.

47. Law Enforcement can search the BitTorrent network in order to locate individuals sharing previously identified child exploitation material in the same way a user searches this network. To search the network for these known torrents can quickly identify targets in their jurisdiction. Law Enforcement receives this information from "Trackers" about peers/clients on the BitTorrent network recently reporting that they are involved in sharing digital files of known or suspected child pornography, based on "info hash" SHA-1 hash values of torrents. These torrents being searched for are those that have been previously identified by law enforcement as being associated with such files. There are BitTorrent network client programs which allow for single-source downloads from a computer at a single IP address, meaning that an entire file or files are downloaded only from a computer at a single IP address as opposed to obtaining the file from multiple peers/clients on the BitTorrent network. This procedure allows for the detection and investigation of those computers

involved in sharing digital files of known or suspected child pornography on the BitTorrent network.

48. During the query and/or downloading process from a suspect BitTorrent network client, certain information may be exchanged between the investigator's BitTorrent client program and the suspect client program they are querying and/or downloading a file from. This information includes 1) the suspect client's IP address; 2) a confirmation from the suspect client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) is being reported as shared from the suspect client program; and 3) the BitTorrent network client program and version being utilized by the suspect computer. Law enforcement has the ability to log this information.

49. The investigation of peer-to-peer file sharing networks is a cooperative effort of law enforcement agencies around the country. Many of these agencies are associated with the Internet Crimes against Children Task Force Program. P2P investigative methodology has led to the issuance and execution of search warrants around the country resulting in the arrest and conviction of numerous offenders possessing and/or distributing child pornography, some of which were also involved in the sexual exploitation of actual child victims.

BACKGROUND OF INVESTIGATION

50. Between October 12 and October 28, 2024, FBI Special Agent Jeffrey Ross was investigating individuals involved in the online sexual exploitation of children via the BitTorrent Network. SA Ross directed his investigative focus to a device (the "Suspect Device"),connected to the Internet from IP Address 24.11.113.97 (the "Subject IP Address,") because it was

associated with a torrent of interest to child pornography investigations. Using a computer running investigative BitTorrent software, he directly connected to the Suspect Device and successfully downloaded 52 files. The Suspect Device reported it was using BitTorrent client software -FW6D32- FrostWire/6.13.3 libtorrent/1.2.19.0.

51. SA Ross reported that one of the files was a text file that was an advertisement for child pornography that stated "2148 FILES 409GBORIGINAL QUALITY VIDEOS, CHILD PORN TEEN SEX INCEST BRO SIS YOUNG GIRLS RUSSIAN TEENS MOMSON PRETEEN HARDCORE PRIVATS".

52. SA Ross reported the majority of the files downloaded were image and video files that depicted prepubescent female children in various states of undress, to include nude posing in sexually explicit poses, engaging in sexual activity with other children, or being sexually abused by adult men and women.

53. For example, SA Ross viewed a downloaded video file titled "51e5db7d72e01aa77dde1c41ccc3e619 - 2012 crying falko girl group man ptsc russiansound woman.mpg" which was approximately six minutes and 46 seconds in length, and depicted small prepubescent female children being vaginally raped, orally sodomized, and anally raped. The video started with the caption "Teach Me To Fuck".

54. On January 16, 2025, an administrative subpoena was served to Comcast to determine the identity of the subscriber assigned the Subject IP Address on the dates and times of the downloads.

55. On January 21, 2025, Comcast identified the subscriber as Jason Knudsen, address 535 27th St Unit 1, Ogden, UT 84403, and provided his telephone number and email address associated with the account. Comcast indicated that Comcast provided internet services

to Knudsen at his residence.

56. Records searches indicated that Knudsen is currently a registered sex offender based on an April, 2013 for attempted sexual exploitation of a minor, a third degree felony in violation of Utah state criminal code 76-5b-201. Sexual Exploitation of a Minor in the Utah state criminal code describes offenses related to the possession and access with intent to view child pornography.

57. After confirming that Knudsen lived at the Odgen address, I sought and obtained federal search warrants for Knudsen's person and home.

58. On February 18, 2025, the search warrant was executed at Knudsen's home in Odgen. Child pornography was found on at least one digital device in his home – a laptop computer. Knudsen, however, was not present. I then went to his workplace to see if he was there. I was informed that he had been arrested on February 13, 2025 by the American Fork Police Department. He was being held at the Utah County Jail, 3075 N Main Street, Spanish Fork, Utah, 84660. FBI Special Agent Jeffrey Ross and I then interviewed Knudsen at the Utah County Jail. Knudsen admitted that he had been engaged in child pornography on the internet. He claimed, however, that the only device that would have child pornography would be the laptop found in his apartment; he said we were welcome to search the Subject Phone but said there would be no child pornographic content on it.

59. On February 19, 2025, I called the Utah County Jail and spoke with Deputy Munoz. I was informed that when Knudsen was arrested, he was in possession of a grey Motorola cellular phone with a black case (the Subject Phone), and that the phone was being stored at the Utah County Jail.

60. The Subject Phone remains at the Utah County Jail with Knudsen's personal

property; it has not been searched. Based on the above, I seek a warrant to search the Subject Phone for violations of the Subject Offenses.

INDIVIDUALS WHO HAVE A SEXUAL INTEREST IN CHILDREN AND RECEIVE AND/OR DISTRIBUTE CHILD PORNOGRAPHY

58. Based on defendant's prior conviction and the current information described above, it appears that Knudsen is someone who possesses, receives, distributes, and/or accesses with intent to view child pornography materials. Based on my previous training and experience related to investigations involving child pornography and the sexual abuse of children, I have learned that individuals, like Knudsen, who create, possess, receive, distribute, or access with intent to view child pornography commonly have a sexual interest in children and in images of children. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to such individuals:

59. The majority of individuals with a sexual interest in children and images of children are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

60. Individuals with a sexual interest in children and images of children collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. These individuals often also collect child erotica, which may consist of images or text that do not rise to the level of child pornography, but which nonetheless fuel their

deviant sexual fantasies involving children. Non-pornographic, seemingly innocuous images of minors are often found on computers and digital storage devices that also contain child pornography, or that is used to communicate with others about sexual activity or interest in children. Such images are useful in attempting to identify actual minors depicted in child pornography images found during the execution of a search warrant. In certain cases, such images may also assist in determining the origins of a particular child pornography image or series of images.

61. Many individuals with a sexual interest in children and images of children will not dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. They regularly maintain their collections in the privacy and security of their homes, cars, garages, sheds, or other secure storage location, such as on their person. Many also often maintain their child pornography collection on mobile digital devices, such as a cellular telephone, so that they can keep their collection easily and securely available wherever they happen to be. Many also frequently delete their collection of child pornography, as well as wipe their digital devices in an attempt to destroy evidence and evade law enforcement.

62. Individuals with a sexual interest in children and images of children often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.

63. Individuals with a sexual interest in children and images of children often maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children, as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

64. Individuals with a sexual interest in children and images of children often collect, read, copy or maintain names, screen names or nicknames, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

65. Based upon training and experience, I know that persons in engaged in the production and possession of child erotica are also often involved in the production and possession of child pornography. Likewise, I know from training and experience that persons involved in the production and possession of child pornography are often involved in the production and possession of child erotica.

66. Based on my training, knowledge, experience, and conversations with others in law enforcement, I understand that an individual who possesses images and/or videos depicting child pornography on one digital storage devices and/or Internet email or online storage account is likely to possess child pornography on additional digital storage devices

and/or Internet email or online storage accounts that s/he possesses. Additionally, based on this training and experience, I understand that an individual who discusses the sexual abuse and/or exploitation of children on one digital storage device is likely to conduct those communications on additional digital storage devices that he possesses. Further, as set forth above, based on my training and experience and my conversations with others in law enforcement, even in the unlikely event that Knudsen has deleted child pornography from his devices, law enforcement can often recover this material with computer forensics. See, for example, paragraph 18 above.

MOBILE DEVICES AND CHILD PORNOGRAPHY

67. Mobile devices such as mobile telephones, smart phones, cellular telephones, and tablets have become an increasingly popular medium used to facilitate the sexual exploitation of children. Mobile devices are relatively small in size (when compared to a laptop or a computer tower). Mobile devices also offer an increasing storage capacity for data, to include pictures and videos. Mobile devices also allow a user to access the Internet through either a data plan, or through free wireless, from anywhere. Mobile devices also allow a user to download any one of several applications which can be used to communicate with others via text, voice, or video. It is also relatively easy for a user to encrypt data on a mobile device or destroy data on a mobile device. A mobile device can also be used to transfer files from one device to another. This can be done by physically connecting a mobile device to a computer and transferring files, removing a mobile device's internal storage (i.e. a micro SD card) and placing it in another device, transferring files wirelessly via a phone's BlueTooth capability, uploading files from the mobile device to a cloud storage account such as Dropbox, Google Drive, or Microsoft OneDrive, or using a mobile device as a wireless hotspot and allowing

other devices (such as a laptop) to connect to the Internet. I know that individuals typically keep a mobile device in an area that they control, typically on their person, in their vehicle, or in their residence.

USE OF BIOMETRICS TO UNLOCK DEVICES

68. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, along with information found in publicly available materials published by device manufacturers, many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features rather than with passwords or passcodes. In light of the foregoing circumstances, during the execution of the search of the Subject Phone described in **Attachment A**, I am seeking specific authorization for law enforcement personnel to compel the use of Knudsen' individual's biometric features. Compulsion of an individual's biometric features includes pressing fingers (including thumbs) against and/or putting a face before the sensor, or any other security feature requiring biometric recognition.[3]

[3] *See Matter of Search of [Redacted] WA, DC*, 317 F.Supp. 3d 523, 527-539 (D.D.C. 2018)(comprehensive analysis and ruling that compulsion of biometric features, as requested in this warrant, violates neither the Fourth Amendment's requirements nor the Fifth Amendment's self-incrimination clause); *In the Matter of the Search of: a White Google Pixel 3 XL Cellphone in a Black Incipio Case*, 398 F.Supp. 3d 785, 789-94 (D. Idaho 2019)(compulsion of biometric features non-testimonial and therefore not violative of suspect's Fifth Amendment right); *In the Matter of the Search of the Search Warrant Application for the Cellular Telephone in United States v. Barrera*, 415 F.Supp. 3d 832, 835-42 (N.D. Ill. 2019)(compulsion of biometric features non-testimonial); *In re Search Warrant No. 5165*, ___ F. Supp. 3d ___, 2020 WL 3581608 (E.D. Ky. 7/2/2020)(adopting and applying D.C. District Court's above decision in striking a warrant's request to compel biometric features from "all individuals" at the premises during the search as overbroad); *but see United States v. Wright*, 431 F. Supp. 3d 1175, 1185-88 (D. Nev. 2020)(unlocking phone with defendant's facial features is testimonial and a violation of Fifth Amendment right); *In the Matter of the Search of a Residence in Oakland, California*, 354 F.

Supp. 3d 1010, 1015-16 (N.D. CA 2019)(utilizing biometric feature to unlock phone is testimonial).

CONCLUSION

69. Based on the investigation described above, probable cause exists to believe that evidence, fruits, and instrumentalities of violations of the Subject Offenses, described in **Attachment B**, will be located in the Subject Phone, described in **Attachment A**.

70. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in **Attachment B**.

/s/ Collin Scott

Collin Scott, Special Agent
Federal Bureau of Investigation

SUBSCRIBED and SWORN before me this 25th day of February, 2025.

The Honorable Cecilia Romero
United States Magistrate Judge

Application for search warrant was reviewed and is submitted by Joey Blanch, Assistant United States Attorney.

ATTACHMENT A

The items to be searched are described as follows:

Motorola Cellular Phone, grey in color with a black case, listed on the personal property of Jason Knudsen, and is currently in possession of the Utah County Jail in Spanish Fork, Utah.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

1. The CELLPHONE or any SD cards themselves if determined that they were used to commit the violations described above.

2. For the CELLPHONE:

   a. evidence of who used, owned, or controlled the CELLPHONE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved user names and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

   b. evidence of software that would allow others to control the CELLPHONE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

   c. evidence of the lack of such malicious software;

   d. evidence indicating how and when the CELLPHONE was accessed or used to determine the chronological context of access, use, and events relating to the crime(s) under investigation and to the device user;

   e. evidence indicating the CELLPHONE user's knowledge and/or intent as it relates to the crime(s) under investigation;

   f. evidence of the attachment to the CELLPHONE of other storage devices or similar containers for electronic evidence;

   g. evidence of programs (and associated data) that are designed to eliminate data from the CELLPHONE;

   h. evidence of the times the CELLPHONE was used;

   i. passwords, encryption keys, and other access devices that may be necessary to access the CELLPHONE;

j. documentation and manuals that may be necessary to access the CELLPHONES or to conduct a forensic examination of the CELLPHONE;

k. records of or information about Internet Protocol addresses used by the CELLPHONE;

l. records of or information about the CELLPHONE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

m. contextual information necessary to understand the evidence described in this attachment.

n. Evidence in any form related to the connection of the CELLPHONE to the Internet.

3. Records, information, and items relating to violations of the statutes described above including:

a. Child pornography, as defined in 18 U.S.C. § 2256(8),

b. Visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);

c. Child erotica, including any materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions;

d. Records, information, and items relating to a sexual interest in children;

e. Records and information tending to identify or locate persons suspected of violating the statutes described above;

f. Records and information tending to identify or locate any children depicted in child pornography or suspected of being sexually exploited in any way;

g. Records and information relating to the sexual exploitation of children, including correspondence and communications between messaging platform users;

h. Records and information showing access to and/or use of Frostwire and any other file sharing program/platform that can be used to receive/distribute/share child pornography;

i. Records and information showing access to and/or use of any website, platform, application, cloud storage, social media account, email account, or messaging account, that can be used to receive/distribute/share child pornography;

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

4. As described above in Attachment B, this warrant allows law enforcement to search for records that might be found in the CELLPHONE, in whatever form they are found. The warrant applied for would authorize the continued seizure of the CELLPHONE and, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

5. There is probable cause to believe those records referenced above will be stored on the CELLPHONE for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Digital files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a digital device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, digital storage media contain electronic evidence of how a device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Digital devices users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

6. As further described in this attachment, this application seeks permission to locate not only digital files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the CELLPHONE were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the CELLPHONE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a

computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating, or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how the device was used, the purpose of its use, who used it, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a digital device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. When an individual uses a digital device to obtain or access child pornography, the individual's device will generally serve both as an instrumentality for committing the crime, and as a storage medium for evidence of the crime. The device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The device is also likely to be a storage medium for evidence of crime. A device used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

7. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant would permit continued seizure, imaging, or otherwise copying of the CELLPHONE and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant. It is intended this warrant will allow for repeated forensic review up to and including the time of trial.